小型／個人企業簡易資安自我評估表

分類	項目	控制說明	未落實(0)	小部份落實(1)	有部份落實(2)	大部份落實(3)	完全落實(4)
系統和設備安全	是否妥善保護存放資料的工具或設備	是否妥善保護存放資料的工具或設備。例如，企業如使用外接設備或 USB 存儲客戶數據，這些工具或設備是否具適當的密碼保護或加密，以防止未經授權的存取或意外丟失，造成客戶數據外流。					
	實施端點保護	端點係指可連接至網路之終端設備，如電腦、手機、平板等。端點保護意味在這些設備上採取適當之安全措施，如安裝防毒軟體、定期更新系統、啟用防火牆，及設定強度密碼，以減少惡意程式或未經授權之人員侵害設備，從而保護企業資料安全。					
	啟用系統稽核日誌	稽核日誌如一本記錄企業系統和資料活動之日誌。它可記錄誰登入系統、何時登入，及曾在系統上進行什麼操作，這些資訊均有助於企業發現異常活動或潛在的威脅。例如有人嘗試多次使用錯誤的密碼登入系統，稽核日誌能記錄這樣的事件並引起管理人員注意。					
	確保雲端服務提供者之安全信譽	當企業使用雲端服務（如 Google Drive、Dropbox 等）儲存資料時，企業應確保所選擇的雲端服務提供商具嚴格之安全措施，如是否提供加密儲存、存取控制、安全備份等，以確保企業在雲端資料安全。					
	適當之管理存取控制權	存取控制意味限制誰可以存取企業資料和系統。例如企業是否僅授權予特定的員工或部門存取部門所屬之敏感資料，或機房設有適當之門禁，避免未經授權之人員存取非屬權限應讀取之資訊，或更動主機。					
	不斷電防護措設	這項控制措施係要求應在儲存企業重要資料的裝置上加置不斷電設備，以避免非預期之停電，造成設備突然中斷致生故障。					
	不使用設備預設密碼	出廠預設密碼如同一把能開啟設備或程式後台的萬能鑰匙。當你更換預設密碼，如同更換這把通用鑰匙，以避免外部第三方使用通用密碼進入設備或程式，提高侵害難度，以保障系統及設備安全。					
資料保護和管理	資料加密	當資料或設備被加密時，就像把訊息轉變成一種難以理解的密碼。沒有正確的解鎖密碼，就無法讀取裡面的內容。企業可使用加密軟體針對機密文件（如 USB、雲端共享文件或郵件附件）進行加密。這樣即使有人未經授權取得文件，也可能需要很長的時間才能解開文件的密碼，因此在短時間內無法瞭解文件內容。					

分類	項目	控制說明	未落實(0)	小部份落實(1)	有部份落實(2)	大部份落實(3)	完全落實(4)
	使用強密碼或多因子驗證	強密碼（通常包含數字、字母和符號的組合）意味一個難以被猜測或破解的密碼；多因子身份驗證則是除了輸入密碼外，還需要另外的驗證方式，例如通過手機收到的驗證碼。透過這樣的方式，提高資料和系統的安全性。					
	資料備份和復原能力	資料備份是確保資料被妥善保存的過程；而資料復原則則關係到企業能否有效地恢復遺失的資料。這意味著企業需要定期備份資料，並擁有能夠有效恢復資料的機制或方法。					
	識別敏感資料並實施保護措施	企業應該清楚識別和分類企業所擁有的敏感資料，例如個人資訊、金融信息等。然後，建立適當的保護措施以確保這些敏感資料得到適當的保護；這些措施可能包括資料是否存儲上鎖的檔案櫃、限制存取權限、或落實桌面淨空等。					
網路和連線安全	安全網路瀏覽和電子郵件	這項控制措施意味著使用安全且可靠的瀏覽器和電子郵件系統，以減少受到網路攻擊或有害程式的風險。例如，使用更新版本的瀏覽器和電子郵件應用程式，並確保它們具有有效的安全功能，例如防毒軟體、反垃圾郵件功能等。					
	考慮應用程式白名單/黑名單	這是一種管理應用程式使用的方法。白名單是指設定允許使用的應用程式清單，而黑名單則是指禁止使用的應用程式清單。這樣做有助於限制員工使用可能具有安全風險的應用程式，從而保護企業資訊安全。					
	使用安全的網路連結	確保企業內部和外部使用的網路連線都是安全的。這可能包括使用加密連線、虛擬私人網路（VPN）等方式，以保護資料在傳輸過程中的安全性，尤其是在使用公共網路時。					
	建立網路區分	企業應視作業需求確認是否將網路分成不同區段，並依此設定不同存取權限。例如將訪客網路和企業內部網路分開，減少外部人員存取企業內部的敏感資料之機率。					
企業策略和風險管理	網路責任保險	這種保險通常涵蓋因資安事件而引起的損失或法律責任。它可以幫助企業應對可能發生的資安事件，例如數據洩露或駭客入侵造成的損失。					
	制定並實施基本標準的網路安全政策文件	企業是否制定符合企業所需之資訊安全政策和規範，並列出企業對於資訊安全的基本標準和要求，例如密碼規範、存取控制等，以幫助員工了解企業對於資訊安全的期望。					
	制定業務連續營運計畫	這是為應對突發事件而制定的計畫，確保企業即使遇到災難或重大中斷也能繼續運作。該計劃通常涵蓋災難恢復、關鍵業務流程回覆、及緊急應變人員的調配等規劃。					

分類	項目	控制說明	未落實(0)	小部份落實(1)	有部份落實(2)	大部份落實(3)	完全落實(4)
	保持系統軟體更新	定期更新系統軟體至最新版本是維持資訊安全的關鍵步驟。這包括作業系統、應用程式的安全性更新，以確保系統及設備已修補已知的安全漏洞。					
	指派角色並定義職責	為不同的人員指定特定的角色和職責，確保資料和權限的適當管理，這有助於減少非經授權存取的機率。					
	參與網路安全資訊共享	參與網路安全資訊共享活動有助於企業獲取和分享相關的安全資訊，這使企業能夠從其他企業的經驗中學習，並掌握最新的安全威脅和解決方案。					
	啟用遠端清除	這是一種安全功能，允許遠程刪除或鎖定遺失或被盜的設備上的敏感資料。當設備遺失或被盜，遠端清除可以防止資料外洩，並確保資料不落入未經授權的人手中。					
	執行網路安全風險評估和測試	定期進行網路安全風險評估和測試有助於識別潛在的弱點和漏洞。這些測試可以模擬攻擊，幫助企業了解其系統和網路存在的安全風險，並採取適當的措施予以修復。					
	定期檢視法律和主管機關規定事項	定期評估法規和監管要求，以確保企業運營符合法律規範。					
	進行員工訓練和測試	給予員工資安培訓並進行定期測試，以驗證其資安意識和應對潛在威脅的能力。這有助於提高員工對資安風險的認識，降低因人為錯誤而導致的安全風險。					

免責聲明

本資安自我評估表僅供參考之用，主要目的係提供無資訊人員配置之小型或個人企業，能初步了解其資訊安全現況之參考。故不應做為一份全面且完整的資安評估，也不應視為專業資訊安全建議或指導，畢竟資安防範應注意要點絕非僅於以上內容。

同時，本資安自我評估表所產生的結果，亦取決於使用者對問題的理解和回答。因此，我們無法對評估表結果的準確性或可靠性作出保證，亦不對由使用此資安自我評估表而產生的任何行動或決策負責。實際執行仍建議應由專業資訊安全專家進一步審核與評估，如您有進一步的資訊安全諮詢或專業建議，建議可尋求資深資訊安全專業人士的協助。